AIR WAR COLLEGE

AIR UNIVERSITY

RESISTANCE IS NOT FUTILE:

THE CASE AGAINST A

CYBER ARMS TREATY

by

Kristine M. Rogers, CIV, USA

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Updated 17 October 2010

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Biography

Kristine Rogers earned her B.A. in International Studies (Law and Diplomacy emphasis, minors in Arabic and Modern Near East Studies) from Brigham Young University, and her M.S. in Computer Science (Computer Security and Information Assurance emphasis) from the George Washington University. In 2002, she began working as an analyst for the US Government. Since that time she has served in a variety of analytic and leadership roles.

Introduction

An inherently flexible medium, cyberspace is controlled more by market forces and popular trends than by formal regulation attempts. Cyberspace is a medium so integrated with modern life that in a growing number of countries it serves as a foundation for many capabilities—including critical infrastructures. Given the lack of security built into the framework of the Internet, it is no surprise that highly connected nation states—those with a heavy reliance on cyber integrated into their critical infrastructures—fear cyber weapons. As a result, nation states desire to impose limits on development of cyber weapons. Since the late 1990s, some states have lobbied for an international cyber arms treaty. [12]

This paper sets out to demonstrate why an international cyber arms treaty is unrealistic option for regulating cyber attack capabilities—in particular, nation state-level cyber weapons. International cyber cooperation on the issue of cyber arms is important; however, a cyber arms control treaty would provide only limited benefit to treaty participants. This paper evaluates the viability of a cyber arms treaty based on its ability to satisfy tactical and strategic factors that would be prerequisites for successful implementation. On the tactical side, participants must agree to provide others with insight into their capabilities, the weapons regulated by the treaty should be measurable, and the treaty's terms must be verifiable. The primary strategic consideration is that the arms treaty should result in limit or reduction of the overall number of cyber arms, thus creating a more secure or stable situation.[3]

A cyber arms treaty would be ineffective due in particular to the lack of a consistent terminology relating to cyber weapons and the indistinct lines between computer network attack and computer network exploitation capabilities. Nation states can easily conceal cyber attack capabilities in the gray area between computer network attack and computer network

exploitation tools. Given the lack of international laws regulating intelligence gathering, it is unlikely that computer network exploitation capabilities—which primarily provide intelligence benefits—would be regulated in a treaty.[4]

Unfortunately, a cyber arms treaty has little hope of either tactical or strategic success. The only realistic benefit might be intelligence gathering on other nations' capabilities; however, even that is of limited utility due to the ease with which states could reveal only those capabilities that they want other states to see—thus creating an opportunity for a deception campaign. This paper also notes how a cyber arms treaty could actually initiate a cyber arms race, instead of promoting disarmament.

Actors in Cyberspace

Cyberspace contains a complex mix of participants, in which the divisions between state actions—those that might fall under a cyber arms treaty—and non-state actions state—ones that may fall under a cyber crimes treaty rather than a cyber arms treaty—are blurry at best. Unlike nuclear and other types of arms development, cyber arms have a low barrier to entry. It is difficult to compare cyber warfare with other forms of warfare, which have a significantly smaller number and range of actors.[56] Governments have little or no control over non-state actors in the cyber realm, who can get involved in production and distribution of cyber arms at little or no cost.

State-level actors

State-level actors range from senior policymakers to intelligence to civilian organizations to military organizations. It is these organizations' activities that may be regulated under a cyber

arms treaty. However, even this is not straightforward. As will be discussed later, the difficulty in distinguishing between computer network attack and computer network exploitation capabilities means that interested parties include—at the very least—military and intelligence organizations, who may disagree about the purpose of cyber arms. Another potential complicating factor is the potential for state sponsored cyber mercenaries—organizations that are not formally part of the government, but which act in accordance with government strategic direction.[78]

While highly connected nation states may be the largest targets of cyber weapons, they would not be the only states targeted for cyber arms regulation. Nation states with less military capability recognize an asymmetric opportunity in the cyber world.[9]

Non-state actors

Even though this paper focuses primarily on state-level actors, it is important to note the role that non-state actors play in complicating the domain.[10] The category of non-state actors includes two general groups: non-state actors with hostile intent, and non-state actors with business motivations. While some hostile non-state actors have financial activities, the distinguishing factors between the two categories is the extent to which the group follows laws, and their intent to cause damage. Hostile non-state actors might include malicious hacker organizations and terrorist groups.[11] Non-state actors with business motivations include private sector businesses, including those companies that support the Internet infrastructure, and general Internet users.[12] Unfortunately, even in the case of non-state actors who follow laws, their technological direction is set more by the market than by the desires of governments.[13]

Malicious and financially-motivated non-state actors may or may not be controlled by their local governments.

Weapons in Cyberspace

Are cyber weapons as dangerous as conventional weapons of mass destruction? The first order effects of cyber weapons do not match the death and destruction that can be caused by nuclear, biological, and other weapons. As a result, aside from requirements for near-real time forensics and attribution, the issue of cyber weapons regulation is significantly different than with other forms of warfare. [14] At present, states do not acknowledge their computer network attack capabilities openly. Unlike nuclear and other weapons of mass destruction, this makes deterrence and coercion difficult, because you cannot tell the extent to which you should fear another state's capabilities.[1516] Also, the rapid pace of development in cyberspace makes it difficult to regulate tools. Today's tools may be obsolete or non-functional tomorrow.

For sake of simplicity, this paper refers both to computer network attack and exploitation tools as "cyber arms" or "cyber weapons." Cyber weapons include software- or hardware-based tools for destroying, disrupting, degrading, or denying access to systems. In particular, cyber arms are those tools which, when used intentionally by state-level actors, create effects that the opponent would view as an act of war in cyberspace. This may include both software that causes the effect, or it could include hardware implants that cause an impact to software.[17]

Discussions of cyber tools and weapons are often divided into two camps: discussion of the tools and their capabilities, or discussion of tools' intended effects.[18] Both descriptions have limitations, in particular because many tools can be used for multiple purposes, and do not neatly fit into either capability- or effects-based categories. Much literature also discusses the

differences between tools designed for the purpose of computer network attack (damaging or destroying data or systems), as opposed to tools whose purpose is computer network exploitation (subverting systems for the purpose of gathering information). Unfortunately, even that model is incomplete, as many tools used for computer network exploitation could also be used as a vehicle for launching attacks.[19]

For the purpose of this discussion, cyber weapons will be divided into two categories: tools that do not require the victim's machine to result in a desired effect, and tools that do require direct access to a victim's machine. This paper focuses more on tools requiring access, because, as discussed later, tools that do not require direct access can be worked around, and the targets can be said to fall under the Law of Armed Conflict.[20]

Cyber Weapons: Direct Access Not Required

The first category of cyber weapons includes those technologies that can cause effects without an attacker having direct access to an adversary's computer systems. In general, these tools can be thought of as the less precise munitions of the Internet. Denial of service weapons—designed to overwhelm computers or networks to prevent them from receiving and transmitting information—are a widely publicized version of this attack.[21] There may be some possibility of categorizing and regulating these tools' tactical use on the battlefield for jamming and related purposes. However, the effects for which these tools are widely known—attacks against commercial systems to cause financial and other damage—may be of limited benefit to the attacker, due to the potential for cross-border spillover. For example, an attack on a US critical infrastructure could impact financial markets worldwide—including the state that launched the attack. Also, while these types of attacks cause temporary damage, eventually

administrators can create workarounds to reestablish access. Other tools in this category include "man in the middle" attacks (altering data mid-stream), and some viruses and worms, which rely on users' own actions to spread the malicious code.

Cyber Weapons: Direct Access Required

The category of cyber weapons requiring direct access to an adversary's computers focuses on more targeted cyber attacks. This category is affected by the blurred border between computer network exploitation and computer network attack tools. Historically, intelligence activities—under which computer network exploitation can be categorized—have not been bound by international treaties. This issue spills into that of computer network attack capabilities. Cyber tools that require "breaking and entry" can fairly easily be asserted to have intelligence gathering capabilities, which would not be regulated under international law.[22]

Cyber arms that require direct access to a machine or system must have a delivery system. While this may sound like an obvious statement, upon further review it demonstrates some of the complexity that would have to be overcome prior to the establishment of a cyber arms treaty. More specifically, attack tools that require direct access and exploitation tools may share some functional capabilities, as well as delivery mechanisms.

Computer Network Exploitation Tools: A Complicating Factor

Effective direct-access computer network attack tools may require the same level of privilege as computer network exploitation tools. In other words, the same tool that is used to infect and gather information from one machine could also be used to launch an attack. This ambiguous line between computer network attack and computer network exploitation tools

makes it difficult to regulate cyber weapons in a consistent and reliable way.[23] This idea can be explored by focusing on the idea of a system administration tool. This is a relevant analogy in particular because some Trojan Horse software—commonly considered malicious software—is also marketed as an inexpensive tool for managing computers across a network. If the software provides a remote user with the right level of access, he or she can either modify or monitor the network.

As with system administration tools, as long as a cyber weapon has the right system access, the user can perform functions that could be categorized either as "attacks" or as "exploitation." If he or she intentionally causes a machine to fail, for example, this action might be considered an attack. If he copies and exports a specific file, that could be considered an exploitation activity. If, however, the exploitation activity also caused a machine to fail, from the vantage point of the victim it might be considered an attack. Forensics may later identify what happened, but it would not necessarily reveal the intent. Perhaps this is why some nation states have indicated that they equate any cyber break-in activities as the equivalent of an "act of war" in cyberspace.

Because nation state espionage activities do not fall under any international treaties, no higher body regulates what is and is not acceptable in information gathering.[24] Even the DoD Joint Publication 3-13 refers to computer network exploitation as an accepted Information Operations capability.[25] Countries have an interest in gathering information from adversaries and competitors. With the worldwide reach that the Internet offers, the Internet becomes a channel for gathering intelligence. This becomes more complicated, as states have an interest or incentive in maintaining their computer network exploitation capabilities. Where those

capabilities overlap with attack capabilities, they will likely categorize the tool in the category not open to treaty verification.

Perishability of Cyber Tools

Another factor that separates cyber tools from kinetic weapons is their perishability. Whereas defenses against nuclear or biological weapons may be difficult to develop, many cyber weapons can be identified and patched quickly. Thus, revealing a capability to a competitor or adversary could provides them with an ability to detect and protect against it, thus obviating the need to have developed the capability in the first place. In addition to patching the now-disclosed vulnerability, they could develop active defense mechanisms to attack their attacker—which may be considered an offensive form of defense.[26]

As indicated earlier, one of the few possible benefits of a cyber arms treaty would be intelligence-related: gaining an understanding of the capabilities that states have developed in the cyber world. Given the current lack of transparency in cyber weapons development, it is reasonable that a state could learn about a capability something that they have not tried themselves. In addition to protecting against it, they could add it to their own research and development efforts. Given the lack of common terminology, they could mix in exploitation capabilities, and it becomes out of the scope of the terms of the treaty. This is a natural behavior in cyberspace research and development: building on ideas observed elsewhere.[27]

In both the case of active defense and integration of an observed capability into new research and development, it is realistic that monitoring of a treaty could itself lead to a cyber tools arms race. Nuclear and chemical weapons do not have a comparable overlap; "dual use" may apply to weapons parts, but generally not to the finished weapon.

The Role of Forensics and Attribution

Attribution of cyber activities—and in particular, states' unwillingness to acknowledge their computer exploitation capabilities and activities—would be a significant barrier to implementing a treaty. The difficulty of identifying perpetrators provides plausible deniability, which state actors would not necessarily want to renounce. First, governments do not want to acknowledge engagement in activities that are considered illegal. Not only is there the potential for negative public opinion, but it could also imply to adversaries that they consent to reciprocal actions at the same level. Finally, revealing or acknowledging cyber capabilities allows an adversary to identify techniques and protect against them.[28] However, even if a source is uncovered, it does not always reveal the intent behind the action.[29]

Goals of Arms Control

Arms control treaties are intended to regulate the development and proliferation of extremely dangerous weapons.[30] The end goal of an arms control agreement is an improved security situation, whether regionally or internationally. The agreement should reduce the risk of war, reduce the cost of preparing for war, and reduce the amount of damage caused should war occur.[31] However, some modern theorists believe that controls over the most dangerous weapons—much less cyber weapons—are obsolete in today's world. Instead, they argue that arms should be controlled in other ways, such as by strategy and the use of instruments of power (diplomatic, informational, military, economic, and cultural initiatives).[32] In the case of cyberspace, this is not possible because there is no single source of control over actors providing

Internet governance. What would be the incentive for these actors to reveal the full range of their cyber capabilities?

Criteria for Success

In order to have a cyber arms control treaty that has some hope of success, a number of tactical and strategic factors must be satisfied under the treaty—including insight, measurability, verifiability, and improvements in international security. A key assumption is that the treaty would not give up a significant amount of sovereignty, in order to maintain some hope of being ratified. If one or more of these factors is not possible, the utility of attempting to create the treaty should be in question.

Tactical Factors for Successful Treaty Implementation

On the tactical side, the parties to the treaty must allow other members to have insight into their efforts, the technology should be measurable, and the terms of the treaty should be verifiable.[33]

Insight

This tactical factor relates to states' willingness to reveal their technological capabilities relating to the regulated technology to an arms control monitoring organizations. If the states involved in the treaty are unwilling to open up their research and design programs for on- or off-site inspection, it is unlikely that a treaty will succeed.[34]

It may be possible to have limited success in convincing states to reveal cyber capabilities to other states. By providing some insight into their activities, they would benefit by gaining an

understanding of other countries' cyber capabilities. This will allow participants to create defenses against other states' capabilities. On the negative side, participants would likely construct the definition of "cyber arms" so as to reveal limited capabilities, but mask other efforts in areas that they can justify as being outside the bounds of the treaty. This allows such activities as computer network exploitation to continue. Additionally, such insight into state level actions does not imply comparable knowledge of corporate activities.[35]

Measurability

Once parties to the treaty are willing to reveal their capabilities, the parties to the treaty and the inspection team should have a clear and consistent understanding of the weapon and its capabilities. They should be able to quantify numbers of weapons in a state's possession, and have some method for comparing one state's capabilities to another. This sounds intuitively obvious, but in the cyber world it is complex. It is not fast or cheap to duplicate a nuclear weapon; it is, however, inexpensive and simple to duplicate a piece of software designed to launch an attack. Nuclear weapons or pathogens are generally easier to define and quantify than software. If the regulated arms are too narrowly defined, this could encourage participant states to make token revelations, without revealing other—perhaps more destructive—capabilities.

Once parties to the treaty are willing to reveal their capabilities, it is important to have an inspection team with an understanding of the weapon's capabilities. They should be able to quantify numbers of weapons in possession, and have some method for comparing one state's capabilities to another. Unfortunately, agreeing on how to measure capabilities and on a definition for measuring a reduction in cyber "stockpiles" is difficult. How does a state "disarm" when copying or archiving parts of a cyber armory is cheap and easy?

As described above, the blurry lines between computer network attack and computer network exploitation tools leads to the potential for token revelations that either reveal capabilities that no longer work, or that deceive other participants about their true capabilities. Scoping the terms of the treaty to exclude tools with computer network exploitation capabilities could have the unintended impact of encouraging states to give the appearance of compliance, while continuing development of attack capabilities.[36] Unfortunately, it is unlikely that exploitation capabilities would be regulated under such a treaty; this means the gap will continue.

Verifiability

In order for the treaty to succeed, treaty verification must be plausible. This not only requires openness and disclosure among parties to the treaty, but also requires an understanding of current and future technologies—specifically, a monitoring organization containing technical experts who are qualified to evaluate capabilities, and compare compliance among countries. They should also possess the ability to assess whether parties may be cheating, or withholding capabilities.[373839]

The question of what would be verified under a cyber arms treaty is also complicated. Does verification include software tools only, or hardware? Would the process include a demonstration of the software, or a full review of program source code? Is it only disclosure of the attack tool, or does it include the delivery mechanism? The latter is significantly impacted by the gray area between computer network attack and exploitation capabilities, because attack and exploitation tools could use the same delivery mechanisms.

Given the rapid pace of changes within the cyberspace domain, treaty verification would require an extremely agile monitoring capability. Considering how quickly computer technology changes, protecting against today's threats would be unlikely to prevent development of future capabilities. Additionally, without reliable attribution, it can be extremely difficult to identify which state-level actors—if any—violated the terms of the treaty. If state-level actors cannot effectively be distinguished from non-state actors, it would be difficult to evaluate compliance; non-state Internet activities could be indistinguishable from state-sponsored activities.

Strategic Factors for Successful Treaty Implementation

The arms treaty should demonstrate a net benefit to participants, vice simply a relinquishing of capability, in order to maintain some hope of approval from individual state governments. This means the treaty must not require participants to give up significant amounts of sovereignty.[40] Without reliable insight, measurability, and verifiability, it would be difficult to convince a government to approve the terms of a treaty. States would be unlikely to become party to the treaty if the treaty terms leave significant room for cheating, or could result in a negative end state—for instance, an arms race rather than arms control.

Strategic Reduction of Capability and Threat

Over time, treaty compliance should result in a quantifiable reduction in the regulated weapons technology, which will produce a more secure and stable international security environment. Parties should maintain sufficient capability to maintain a sense of security, but the overall international threat diminishes.[41] Unfortunately, a cyber arms treaty would likely not lead to any significant change. Parties to the treaty would probably continue to engage in

development of dual use technologies—specifically, computer network exploitation tools with computer network attack capabilities, or potential for such capabilities. Over time, the treaty would not result in a reduction of cyber threats even at the state level, much less over non-state actors.

In theory, monitoring is not about intelligence gathering. However, participants cannot discount the possibility that participants report back to intelligence services. As described earlier, when states reveal their cyber capabilities during the verification process, they could unintentionally be providing others with ideas about how to expand programs. In fact, the likelihood of a cyber arms treaty providing security and disarmament is so low that it may even be more likely that such a treaty would start vice prevent a cyber arms race.

The very notion of cyber disarmament is problematic in a world where copying files is very simple. What qualifies as disarmament? Provision of patches against states' capabilities? Or is it deletion of files? If the file is deleted, how do you prove the file is gone? An actor could easily modify a file slightly before using it again.[42]

Benefits of a Cyber Arms Treaty

Despite the fact that a cyber security treaty would likely be ineffective, some states support the notion of a treaty. What, then, could a state gain from a cyber arms treaty? The primary benefit of a cyber arms treaty would be intelligence, not security. It would allow states to understand other states' capabilities, and gauge overall sophistication levels. Through this insight, states would be able to design defenses and countermeasures against those tools revealed by the other parties to the treaty—though, as emphasized above, these capabilities may not represent the state's actual range of abilities. Through this understanding of others' capabilities,

states may be able to assess whether they have a relative advantage, and possibly be able to use their capability to deter or coerce. Finally, participation in such a treaty creates opportunities for states to run information operations against one another, misleading other states into believing their capabilities are at a different level.

Costs of a cyber arms treaty

On the other hand, revealing cyber capabilities—even if not a full disclosure—quickly leads to a loss of the disclosed capabilities. This is much more extreme than with the types of treaties to which cyber arms have been compared. In cyberspace, the cycle of identifying a vulnerability, creating an exploit, discovering the exploit, and patching against the exploit can be very fast. Another potential cost is the fact that there would be no guarantee that the other participants have shared the breadth of their capabilities; in fact, the dual nature of computer network exploitation and attack tools would make it simple to limit participation to token revelations. Finally, because the technology changes rapidly, participants may be able to regulate some of today's weapons, but not tomorrow's weapons. It would be difficult to categorize cyber weapons in broad enough terms that a treaty developed today remains relevant tomorrow.

Future Directions

At present, many obstacles would have to be removed in order to create a situation in which a cyber arms treaty could be considered viable. First, the international community would need to agree upon a common terminology for warfare in cyberspace. This would include an internationally accepted and enforceable definition of cyber weapons, agreement on thresholds

defining acts of war in cyberspace—for instance, what would be seen as an act that could justify a kinetic retaliation—and agreement on whether civilian or non-state actions, which may or may not be state sponsored, can be interpreted as acts of war. States also would have to agree to show their capabilities before can even come to the table to create a cyber arms treaty.

Second, both technical and political progress would have to be made on the topic of attribution. Victims require technical means to identify when a cyber attack has occurred. Then, the victim needs a technical ability for determining where the attack originated—which can be an extremely difficult task. States that launched the attack would have to be willing to admit responsibility for the attack as appropriate.

Third, a cyber arms regulatory agency would have to be established. Such an organization would not fit neatly into existing Internet organizations, which focus on commercial and technological development priorities. It may be possible to create a new organization under an internationally accepted body, such as the United Nations.

As an alternative to regulating weapons under a cyber arms treaty, it may be more worthwhile to create an international agreement on categories of acceptable cyber targets. This would not, however, be a treaty—rather, the Law of Armed Conflict already applies to this discussion. One potentially effective international discussion would be mapping cyber threats and activities to the Law of Armed Conflict.[4344] Lawyers and military officials around the world have presented theories on how the Law of Armed Conflict applies in cyberspace; coming to international consensus on this topic could pave the way for future agreements on cyberspace.[4546]

Conclusion

At present, a cyber arms treaty is infeasible. By evaluating the potential for success using the model identified above—tactical and strategic implementation—it appears that a treaty on cyber weapons would be likely to fail. It may be possible to achieve partial success on insight and measurability, but the other factors have little or no chance of success under the current cyberspace environment. Other forms of agreements would provide a more tangible benefit, and could pave the way for a future agreement such as a treaty. In particular, one possible positive action is achieving an international agreement on how the Law of Armed Conflict applies to cyber activities and targets.

The inherent anarchic nature of the Internet makes it difficult to regulate; when analyzed according to the tactical and strategic criteria, it is clear that a cyber arms treaty would not be an effective measure for controlling cyber threats. A cyber arms treaty could not serve as anything more than a token agreement—something that shows a willingness to cooperate on cyber issues, without agreeing to any significant change.[47][48]

Bibliography

Adams, James. *The Next World War: Computers Are the Weapons and the Front Line Is Everywhere.* New York: Simon and Schuster, 1998.

Adelman, Kenneth L. "Arms Control with and without Agreements." *Foreign Affairs* 63, no. 2 (Winter 1984): 240-263.

Arquilla, John, and David Ronfeldt. *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica, CA: RAND, 1997.

Arwood, Sam. *Cyberspace as a Theater of Conflict: Federal Law, National Strategy and the Departments of Defense and Homeland Security.* AFIT, 2007.

Campen, Alan D., and Douglas H. Dearth, . *Cyberwar 2.0: Myths, Mysteries and Reality.* Fairfax, VA: AFCEA International Press, 1998.

Campen, Alan D., and Douglas H. Dearth, . *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict.* Fairfax, VA: AFCEA International Press, 2000.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld.* ???: O'Reilly Media, 2009.

Denning, Dorothy E. *Information Warfare and Security.* New York: ACM Press, 1999.

—. "Obstacles and Options for Cyber Arms Controls." *Arms Control in Cyberspace.* Berlin, Germany: Heinrich Böll Foundation, June 29-30, 2001.

Denning, Dorothy E. "Reflections on Cyberweapons Controls." *Computer Security Journal* XVI, no. 4 (Fall 2000): 43-53.

Emery, Norman E. "Irregular Warfare Information Operations: Understanding the Role of People, Capabilities, and Effects." *Military Review*, Nov-Dec 2008: 27-38.

Gallagher, Nancy W. *The Politics of Verification.* Baltimore, MD: The Johns Hopkins University Press, 1999.

Gray, Colin S. *Modern Strategy.* New York: Oxford University Press, 1999.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. *Information Warfare and International Law.* Vienna, VA: National Defense University Press, 1997.

Hester, D. Micah, and Paul J. Ford. *Computers and Ethics in the Cyberage.* Upper Saddle River, NJ: Prentice Hall, 2001.

JP 3-13: Information Operations. US Joint Publication, 13 February 2006.

Karresand, Martin. *A Proposed Taxonomy of Software Weapons.* Swedish Defence Research Agency, 2003.

Kent, Glenn A. *Thinking about America's Defense.* Santa Monica, CA: RAND, 2008.

Khalilzad, Zalmay M., and John P. White. *The Changing Role of Information in Warfare.* Santa Monica, CA: RAND, 1999.

Kramer, Franklin D., Stuart H. Starr, and Larry Wentz. *Cyberpower and National Security.* Dulles, VA: Potomac Books, Inc., 2009.

Larsen, Jeffrey A., and James J. Wirtz. *Arms Control and Cooperative Security.* Boulder, CO: Lynne Rienner Publishers, Inc., 2009.

Lennon, Alexander T. J., ed. *Contemporary Nuclear Debates.* Cambridge, MA: The Center for Strategic and International Studies, 2002.

Levi, Michael A., and Michael E. O'Hanlon. *The Future of Arms Control.* Washington, D.C.: Brookings Institution Press, 2005.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare.* New York: Cambridge University Press, 2007.
—. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND, 2009.
—. *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon.* Washington, D.C.: U.S. Government Printing Office, 1994.
Lonsdale, David J. *The Nature of War in the Information Age.* New York: Frank Cass, 2004.
Muller, Harald. "Compliance Politics: A Critical Analysis of Multilateral Arms Control Treaty Enforcement." *The Nonproliferation Review,* Summer 2000: 77-90.
Owens, William A., Kenneth W. Dam, and Herbert S. Lin. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, D.C.: The National Academies Press, 2009.
Pendall, Major David W. "Effects-Based Operations and the Exercise of National Power." *Military Review*, January-February 2004: 20-31.
Rattray, Gregory J. *Strategic Warfare in Cyberspace.* Boston, MA: The MIT Press, 2001.
Stein, George. *Information War – Cyberwar – Netwar.* Vol. Air War College Studies in National Security No.3, in *Battlefield of the Future: 21st Century Warfare Issues*, edited by Barry R. Schneider and Lawrence E. Grinter, 153-170. Montgomery, AL: Air University, 1995.
Wingfield, Thomas C. "Legal Aspects of Offensive Information Operations in Space." *Journal of Legal Studies* 9 (1998-1999): 121-145.
Wingfield, Thomas C., and James B. Michael. *An Introduction to Legal Aspects of Operations in Cyberspace.* Monterey, CA: Naval Postgraduate School, 2004.

End Notes

[1] Denning, Reflections on Cyberweapons Controls Fall 2000, 11
[2] Denning, Obstacles and Options for Cyber Arms Controls June 29-30, 2001
[3] Larsen and Wirtz 2009, 6-11
[4] Denning, Obstacles and Options for Cyber Arms Controls June 29-30, 2001
[5] Denning, Reflections on Cyberweapons Controls Fall 2000, 8
[6] Denning, Reflections on Cyberweapons Controls Fall 2000, 8
[7] Libicki, Cyberdeterrence and Cyberwar 2009, 98-102
[8] Denning, Information Warfare and Security 1999, 25-28
[9] Kramer, Starr and Wentz 2009, 287
[10] Kramer, Starr and Wentz 2009, 338
[11] Libicki, Cyberdeterrence and Cyberwar 2009, 28
[12] Libicki, Conquest in Cyberspace: National Security and Information Warfare 2007, 148-166
[13] Campen and Dearth, Cyberwar 2.0: Myths, Mysteries and Reality 1998, 295-312
[14] Levi and O'Hanlon 2005, 87-92
[15] Libicki, Cyberdeterrence and Cyberwar 2009, 39-41, 52-71
[16] Kramer, Starr and Wentz 2009, 309-340
[17] Gray 1999, 249-251
[18] Denning, Reflections on Cyberweapons Controls Fall 2000, 1-2
[19] Libicki, Conquest in Cyberspace: National Security and Information Warfare 2007, 28-29
[20] Greenberg, Goodman and Hoo 1997
[21] Kramer, Starr and Wentz 2009, 446-447
[22] Denning, Obstacles and Options for Cyber Arms Controls June 29-30, 2001, 8
[23] Libicki, Cyberdeterrence and Cyberwar 2009, 23-27
[24] Greenberg, Goodman and Hoo 1997, 24-25
[25] JP 3-13: Information Operations 13 February 2006
[26] Denning, Obstacles and Options for Cyber Arms Controls June 29-30, 2001, 4
[27] Denning, Obstacles and Options for Cyber Arms Controls June 29-30, 2001, 4
[28] Libicki, Cyberdeterrence and Cyberwar 2009, 75-93
[29] Denning, Obstacles and Options for Cyber Arms Controls June 29-30, 2001, 9
[30] Levi and O'Hanlon 2005, 9
[31] Larsen and Wirtz 2009, 9-10, 22-23, 39-40
[32] Gray 1999, 193-195
[33] Denning, Obstacles and Options for Cyber Arms Controls June 29-30, 2001, 2
[34] Gallagher 1999, 8, 11, 35
[35] Libicki, Cyberdeterrence and Cyberwar 2009, 75-90
[36] Libicki, Cyberdeterrence and Cyberwar 2009, 91-103
[37] Gallagher 1999, 9, 38-42
[38] Levi and O'Hanlon 2005, 63-67
[39] Larsen and Wirtz 2009, 88-89
[40] Gallagher 1999, 4-5, 8-9
[41] Larsen and Wirtz 2009, 9-10, 24
[42] Denning, Obstacles and Options for Cyber Arms Controls June 29-30, 2001, 3
[43] Denning, Obstacles and Options for Cyber Arms Controls June 29-30, 2001, 7
[44] Greenberg, Goodman and Hoo 1997, 93-103
[45] Kramer, Starr and Wentz 2009, 525-542
[46] Wingfield, Legal Aspects of Offensive Information Operations in Space 1998-1999
[47] Denning, Obstacles and Options for Cyber Arms Controls June 29-30, 2001

[48] Denning, Reflections on Cyberweapons Controls Fall 2000